UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,606	08/21/2003	Vincent J. Zimmer	42.P16845	9801

7590 06/04/2007

R. Alan Burnett
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
06/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/646,606	ZIMMER ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20070308*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 08 March 2007. By this response, Claims 1, 17, and 27 have been amended. No claims have been added or canceled. Claims 1-30 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 08 March 2007 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 17-26 under 35 U.S.C. 101 as directed to non-statutory subject matter, Applicant argues that the amendments to Claim 17 render the claims directed to statutory subject matter (page 11 of the present response). The Examiner respectfully disagrees. Specifically, the Examiner notes that there is no support or written description for the term "tangible machine readable medium" in the present specification. Without such written description, it is not clear exactly which media would be encompassed by the term tangible, and it appears that various forms of machine readable media would be tangible but still not statutory in terms of providing a functional interrelationship between the medium and any data or instructions stored on the medium. See MPEP § 2106.01.

Regarding the applicability of Hsu, US Patent Application Publication 2005/0081036, Applicant alleges that Hsu does not qualify as prior art under any

section of 35 U.S.C. 102 and therefore cannot be used as a reference in a rejection under 35 U.S.C. 103 (page 14 of the present response). The Examiner respectfully disagrees. Specifically, although the actual filing date of Hsu is later than the filing date of the present application, the effective filing date of Hsu is earlier than the filing date of the present application, taking into account the claim to the benefit of a prior U.S. application under 35 U.S.C. 120. Therefore, Hsu qualifies as prior art under 35 U.S.C. 102(e). See MPEP § 706.02(f)(1).

3. Applicant's arguments with respect to the rejections of claims 1-30 under 35 U.S.C. 102(e) and 103(a) have been considered but are moot in view of the new ground(s) of rejection.

Specification

4. The disclosure is objected to because of the following informalities:

The specification contains an embedded hyperlink and/or other form of browser-executable code (see page 14, line 9, in paragraph 0044). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Appropriate correction is required. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors.

Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 17 has been amended to recite a "tangible machine-readable medium"; however, the specification does not provide proper antecedent basis for such a limitation. See below regarding the rejection under 35 U.S.C. 112, first paragraph, for further detail.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 17-26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, on page 25, paragraph [0074] of the specification, Applicant provides, "... a machine-readable medium may include propagated signals such as electrical... or other form of propagated signals (e.g., carrier waves, infrared signals...)." Signals do not fall under any of the statutory classes of invention; a signal is neither a process, a machine, an article of manufacture, nor a composition of matter. Therefore, because the claims encompass both statutory and

non-statutory subject matter, the claims as a whole are considered to be directed to non-statutory subject matter.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 17-26 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Specifically, Claim 17 has been amended to recite the limitation "a tangible machine-readable medium". Although the specification describes various examples of machine-readable media, none is explicitly described as a tangible medium, nor does there appear to be any mention of the term "tangible" whatsoever. It is not clear exactly which of the examples provided in the specification are intended to be encompassed by the new limitation. Therefore, there is not sufficient written description of the subject matter of Claim 17 as amended.

Claims 18-26 are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-4, 9-18, 24-28, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al, US Patent 6976163, in view of Rakavy et al, US Patent 5978912.

In reference to Claim 1, Hind discloses a method that includes issuing, via a caller computer, a request to have a firmware service be performed via firmware on a remote computer (col. 6, lines 4-19 and lines 53-55); authenticating the caller computer (col. 11, lines 8-11; col. 13, lines 39-56); and performing the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service (col. 13, lines 39-63). However, Hind does not explicitly disclose that the firmware service includes executing program code included in the firmware under control of the caller computer.

Rakavy discloses a method in which a calling computer requests to have a firmware service be performed, where the firmware service includes executing program code in the firmware under control of the calling computer (see column 13, lines 42-60, where remote procedure calls are made from the calling computer to the BIOS of another remote computer) and the communications between the calling computer and

the remote computer can be authenticated (see column 9, lines 51-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hind to include the firmware service as described by Rakavy, in order to allow communication with a remote computer without needing to use the computer's operating system (see Rakavy, column 3, line 66-column 4, line 14).

In reference to Claim 2, Hind and Rakavy further disclose initializing a listening mechanism on the remote computer to receive the request (Hind, col. 9, lines 37-52; col. 10, lines 8-24).

In reference to Claim 3, Hind and Rakavy further disclose that the listening mechanism is interrupt-based, further comprising asserting an interrupt on a processor of the remote computer in response to receiving the request (Hind, col. 9, lines 37-52; col. 10, lines 8-24 – hardware latch can interrupt).

In reference to Claim 4, Hind and Rakavy further disclose that the listening mechanism is polling-based, and the method also includes periodically polling a network interface of the remote computer to determine if the remote computer has received a request (Hind, col. 6, lines 4-19; col. 9, lines 37-52; col. 10, lines 8-24 – update capability of programmable memory is enabled and therefore would await an update signal from a caller computer).

In reference to Claim 9, Hind and Rakavy further disclose issuing at least one authentication certificate to the remote computer, each of said at least one authentication certificate containing authentication information corresponding to a respective caller computer (Hind, col. 12, lines 12-29; col. 15, line 57 – col. 16, line 45);

receiving authentication credentials from a caller computer (Hind, col. 12, lines 12-29; col. 15, line 57 – col. 16, line 45); authenticating the caller computer via the authentication credentials in view of a corresponding authentication certificate from among said at least one authentication certificate issued to the remote computer (Hind, col. 12, lines 12-29; col. 15, line 57 – col. 16, line 45; Rakavy, column 9, lines 51-60).

In reference to Claim 10, Hind and Rakavy further disclose determining if an authentication certificate corresponding to the caller computer has expired (Hind, col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31 – firmware release level in certificate would determine expiration).

In reference to Claim 11, Hind and Rakavy further disclose determining if an authentication certificate corresponding to the caller computer has been revoked (Hind, col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31 – update flag set to "NO" indicates revocation).

In reference to Claim 12, Hind and Rakavy further disclose authenticating the remote computer (col. 6, lines 4-19; col. 10, line 60 – col. 11, line 14; col. 12, line 45 – col. 13, line 12; Rakavy, column 9, lines 51-60).

In reference to Claim 13, Hind and Rakavy further disclose sending encrypted traffic relating to the firmware service request and results of the request between the caller computer and the remote computer (Hind, col. 12, lines 22-44; col. 13, line 39 – col. 14, line 39).

In reference to Claim 14, Hind and Rakavy further disclose performing a cipher negotiation between the caller computer and the remote computer to agree upon an

encryption technique used to encrypt and decrypt the encrypted traffic (Hind, col. 10, line 60 – col. 11, line 14).

In reference to Claim 15, Hind and Rakavy further disclose that the encryption technique employs at least one session key (Hind, col. 10, line 60 – col. 11, line 14; col. 11, lines 19-31 – special key; Rakavy, column 9, lines 51-60).

In reference to Claim 16, Hind and Rakavy further disclose that communications between the caller computer and the remote computer are performed using an out-of-band communication channel that operates independent of an operating system to run or running on the remote computer (Rakavy, column 3, line 66-column 4, line 3, where communications do not utilize the computer's operating system).

In reference to Claim 17, Hind discloses a medium storing software instructions that instruct a processor to receive a request from a caller computer to perform a firmware service (col. 6, lines 4-19 and lines 53-55); authenticate the caller computer (col. 11, lines 8-11; col. 13, lines 39-56); and perform the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service (col. 13, lines 39-63). However, Hind does not explicitly disclose that the firmware service includes executing program code included in the firmware under control of the caller computer.

Rakavy discloses a method in which a calling computer requests to have a firmware service be performed, where the firmware service includes executing program code in the firmware under control of the calling computer (see column 13, lines 42-60,

where remote procedure calls are made from the calling computer to the BIOS of another remote computer) and the communications between the calling computer and the remote computer can be authenticated (see column 9, lines 51-60), and further that communications between the caller computer and the remote computer are performed using an out-of-band communication channel that operates independent of an operating system to run or running on the remote computer (column 3, line 66-column 4, line 3, where communications do not utilize the computer's operating system). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the program of Hind to include the firmware service as described by Rakavy, in order to allow communication with a remote computer without needing to use the computer's operating system (see Rakavy, column 3, line 66-column 4, line 14).

In reference to Claim 18, Hind and Rakavy further disclose that execution of the plurality of instructions further performs the operation of initializing a listening mechanism to receive the request (Hind, col. 9, lines 37-52; col. 10, lines 8-24).

In reference to Claim 24, Hind and Rakavy further disclose a firmware storage device and the plurality of instructions comprise firmware (Hind, col. 6, line 64 – col. 7, line 16).

In reference to Claim 25, Hind and Rakavy further disclose that execution of the plurality of instructions further performs the operation of performing a cipher negotiation between the caller computer and a remote computer on which the plurality of instructions are executed to agree upon an encryption technique to be used to encrypt

and decrypt encrypted traffic to be sent between the caller computer and the remote computer (Hind, col. 10, line 60 – col. 11, line 14).

In reference to Claim 26, Hind and Rakavy further disclose that the encryption technique employs a shared asymmetric session key (col. 10, line 60 – col. 11, line 14; col. 11, lines 19-31; Rakavy, column 9, lines 51-60).

In reference to Claim 27, Hind discloses a computer system including a processor and a memory operatively coupled to the processor (col. 6, line 64 – col. 7, line 16); a network interface operatively coupled to the processor (col. 8, lines 8-20); and at least one flash device operatively coupled to the processor on which firmware instructions are stored, which when executed by the processor perform operations (col. 6, line 64 – col. 7, line 16; col. 8, lines 33-63) that include receiving a request to perform a firmware service received from a caller computer via the network interface (col. 6, lines 4-19 and lines 53-55); authenticating the caller computer (col. 11, lines 8-11; col. 13, lines 39-56); and performing the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service (col. 13, lines 39-63). However, Hind does not explicitly disclose that the firmware service includes executing program code included in the firmware under control of the caller computer.

Rakavy discloses a method in which a calling computer requests to have a firmware service be performed, where the firmware service includes executing program code in the firmware under control of the calling computer (see column 13, lines 42-60, where remote procedure calls are made from the calling computer to the BIOS of

another remote computer) and the communications between the calling computer and the remote computer can be authenticated (see column 9, lines 51-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Hind to include the firmware service as described by Rakavy, in order to allow communication with a remote computer without needing to use the computer's operating system (see Rakavy, column 3, line 66-column 4, line 14).

In reference to Claim 28, Hind and Rakavy further disclose that execution of the firmware instructions performs the further operation of periodically polling the network interface to determine if the network interface has received a request from a caller computer to perform a firmware service (Hind, col. 6, lines 4-19; col. 9, lines 37-52; col. 10, lines 8-24).

In reference to Claim 30, Hind and Rakavy further disclose that execution of the firmware instructions further performs the operation of performing a cipher negotiation between the caller computer and the computer system to agree upon an encryption technique to be used to encrypt and decrypt encrypted traffic to be sent between the caller computer and the computer system (Hind, col. 10, line 60 – col. 11, line 14).

12. Claims 5-8, 19-23, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind in view of Rakavy as applied to claims 1, 17, and 27 above, and further in view of Hsu, US Patent Application Publication 2005/0081036.

In reference to Claim 5, Hind and Rakavy disclose everything as applied above to Claim 1, and further generally disclose performing authentication (Rakavy, column 9,

lines 51-60); however, neither Hind nor Rakavy explicitly discloses issuing an authentication challenge to the caller computer; and evaluating a response by the caller computer to the authentication challenge. Hsu discloses issuing an authentication challenge to the caller computer (paragraphs [0039]-[0047]); and evaluating a response by the caller computer to the authentication challenge (paragraphs [0039]-[0047]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Hind and Rakavy with Hsu's key generation system utilizing an authentication challenge to use other encryption methods. It is for this reason that one of ordinary skill in the art would have been motivated to provide an authentication challenge because it minimizes the amount of traffic sent and increase the frequency of challenges (Hsu, paragraph [0033]).

In reference to Claim 6, Hind, Rakavy, and Hsu further disclose encrypting original data using a first key held by the remote computer to create encrypted original data (Hind, col. 10, lines 51-67; col. 14, lines 15-39); sending the encrypted original data to the calling computer (Hind, col. 12, lines 12-63); decrypting the encrypted original data using a second key held by the caller computer to create decrypted data (Hind, col. 6, lines 4-19; col. 12, lines 12-63); sending the decrypted data back to the remote computer (Hind, col. 6, lines 4-19; col. 12, line 12 – col. 13, line 12); and comparing the decrypted data with the original data to authenticate the calling computer (Hind, col. 12, lines 34-36).

In reference to Claim 7, Hind, Rakavy, and Hsu further disclose extracting the first key from an authentication certificate for the caller computer issued to the remote computer (Hind, col. 13, lines 48-52).

In reference to Claim 8, Hind, Rakavy, and Hsu further disclose that the first key is an public key contained in the authentication certificate and the second key comprises a private key held by the calling computer that is the asymmetric key for the public key (Hind, col. 12, lines 22-32 and lines 56-63; col. 13, lines 48-52).

In reference to Claim 19, Hind and Rakavy disclose everything as applied above to Claim 17, and further generally disclose performing authentication (Rakavy, column 9, lines 51-60); however, neither Hind nor Rakavy explicitly discloses issuing an authentication challenge to the caller computer; receiving a response to the authentication challenge from the caller computer; and evaluating a response by the caller computer to the authentication challenge. Hsu discloses issuing an authentication challenge to the caller computer (paragraphs [0039]-[0047]); receiving a response to the authentication challenge from the caller computer (paragraphs [0039]-[0047]); and evaluating a response by the caller computer to the authentication challenge (paragraphs [0039]-[0047]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the software of Hind and Rakavy with Hsu's key generation system utilizing an authentication challenge to use other encryption methods. It is for this reason that one of ordinary skill in the art would have

been motivated to provide an authentication challenge because it minimizes the amount of traffic sent and increase the frequency of challenges (Hsu, paragraph [0033]).

In reference to Claim 20, Hind, Rakavy, and Hsu further disclose that evaluating the response to the authentication challenge includes extracting authentication credentials for the caller computer contained in the response (Hsu, paragraphs [0043]-[0044]); identifying an authentication certificate corresponding to the caller computer (Hind, col. 12, lines 12-29; col. 13, lines 39-56); and checking authentication credentials for the caller computer against the authentication certificate that is identified (Hind, col. 12, lines 12-29; col. 13, lines 39-56).

In reference to Claim 21, Hind, Rakavy, and Hsu further disclose that execution of the plurality of instructions further performs the operation of determining if the authentication certificate that is identified has expired (Hind, col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31).

In reference to Claim 22, Hind, Rakavy, and Hsu further disclose that execution of the plurality of instructions further performs the operation of determining if the authentication certificate that is identified has been revoked (Hind, col. 12, lines 45-56; col. 14, lines 40-54; col. 17, lines 25-31).

In reference to Claim 23, Hind, Rakavy, and Hsu further disclose that execution of the plurality of instructions performs further operations including generating a random number (Hsu, paragraphs [0033], [0041], [0044]); encrypting the random number using a first key to create an encrypted random number (Hsu, paragraph [0044]); sending the encrypted random number to the calling computer (Hsu, paragraphs [0043]-[0044]);

receiving decrypted data derived from the encrypted random number from the calling computer (Hsu, paragraphs [0043]-[0044], [0053]) comparing the decrypted data with the random number to authenticate the calling computer (Hsu, paragraph [0041]).

In reference to Claim 29, Hind and Rakavy disclose everything as applied above to Claim 17, and further generally disclose performing authentication (Rakavy, column 9, lines 51-60); however, neither Hind nor Rakavy explicitly discloses issuing an authentication challenge to the caller computer; receiving a response to the authentication challenge from the caller computer; and evaluating the response to determine whether the caller computer is authenticate. Hsu discloses issuing an authentication challenge to the caller computer (paragraphs [0039]-[0047]); receiving a response to the authentication challenge from the caller computer (paragraphs [0039]-[0047]); and evaluating the response to determine whether the caller computer is authenticated (paragraphs [0039]-[0047]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the system of Hind and Rakavy with Hsu's key generation system utilizing an authentication challenge to use other encryption methods. It is for this reason that one of ordinary skill in the art would have been motivated to provide an authentication challenge because it minimizes the amount of traffic sent and increase the frequency of challenges (Hsu, paragraph [0033]).

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER